Department of Homeland Security Daily Open Source Infrastructure Report for 20 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports passengers in Reagan National Airport were evacuated on Thursday, March 16, after a security breach when a passenger got through the security checkpoint with a boxcutter. (See item 17)
- The Washington Post reports the government's effort to develop a new anthrax vaccine has run into difficulty, with the company in charge of the project reporting failure in a major human test and falling at least a year behind schedule. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 17, New York Times* — **Nuclear reactors found to be leaking radioactive water.** The public's acceptance of new nuclear reactors depends in part on the performance of the old ones, and lately several of those have been discovered to be leaking radioactive water into the ground. Near Braceville, IL, the Braidwood Generating Station, owned by the Exelon Corporation, has leaked tritium into underground water that has shown up in the well of a family nearby. The company, which has bought out one property owner and is negotiating with others, has offered to help pay for a municipal water system for houses near the plant that have private wells. In a survey of all 10 of its nuclear plants, Exelon found tritium in the ground at

two others. On Tuesday, March 14, it said it had had another spill at Braidwood, about 60 miles southwest of Chicago, and on Thursday, March 16,the attorney general of Illinois announced she was filing a lawsuit against the company over that leak and five earlier ones, dating to 1996. Also, in New York, at the Indian Point 2 reactor in Buchanan, workers digging a foundation adjacent to the plant's spent fuel pool found wet dirt, an indication that the pool was leaking. New monitoring wells are tracing the tritium's progress toward the Hudson River.
Source: http://www.nytimes.com/2006/03/17/national/17nuke.html?_r=1&pagewanted=all&oref=slogin

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *March 17, CBS 3 (NJ)* — **Overturned semi creates Hazmat scare in New Jersey.** An overturned semi, carrying household cleaning products, brought traffic to a crawl in the southbound lanes of the New Jersey Turnpike Friday morning, March 17. Lanes were reopened later that afternoon.
   Source: http://cbs3.com/local/local_story_076094444.html

3. *March 17, Toledo Blade (OH)* — **Possible leak at plant spurs evacuation in Ohio.** RemTec International, a manufacturing plant, and the surrounding area in Bowling Green, OH, were evacuated Thursday night, March 16, because of a possible gas leak, authorities said. Bowling Green police and fire crews set up a safe zone and asked those in the area to remain in their homes. A shelter was set up for those wanting to evacuate.
   Source: http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20060317/NEWS17/60317014/−1/NEWS

4. *March 17, Richmond Times−Dispatch (VA)* — **Chemical firm, neighborhood evacuated in Virginia.** Employees of a chemical company located east of Defense Supply Center in Richmond, VA, and residents of nearby Crest Hill trailer park were evacuated at midday Friday, March 17, after about 150 gallons of nitric acid spilled onto the ground at Industrial Chemicals Inc. The spill was caused by a faulty valve.
   Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&%09s=1045855935074&c=MGArticle&cid=1137834785927&path=%21news%21localupdates

5. *March 17, WAOW (WI)* — **Gas tanker explosion prompts highway closure in Wisconsin.** A semi−tanker carrying 8,700 of gallons of gasoline exploded Friday morning, March 17, on Wisconsin Highway−29, shutting down the road for more than seven hours. Only a metal frame was left of a Rieser Energy semi−tanker after it exploded. Shawano County fire departments fought the fire for several hours.
   Source: http://www.waow.com/news/full_story.php?id=39950

[Return to top]

Defense Industrial Base Sector

6. *March 17, New York Times* — **Fighter jet partners pressure the Pentagon to share more of its critical technology.** The F−35 Joint Strike Fighter −− a $256 billion fighter jet program led by the U.S. and co−financed by eight allied nations −− was supposed to be a model of international cooperation. But because of American reluctance to share critical technologies, some of the biggest partners are threatening to withdraw. Last week, Britain, the principal foreign partner in the program to build the next−generation radar−evading supersonic jet, delivered an ultimatum at a Senate Armed Services Committee hearing. Lord Peter Drayson, Britain's top weapons buyer, said Britain would withdraw from the program unless it gained better access to software technology and stealth technology needed to maintain and upgrade the planes it buys. Meanwhile, five other nations that are partners in the project −− Norway, Italy, Turkey, Denmark and the Netherlands −− met Friday, March 10, in the Netherlands to lay the groundwork for a united front to deal with the Pentagon. While much of the complaining seems aimed at better working terms with the U.S., the new government in Norway is questioning whether the country should remain in the program. Along with Canada and Australia, these foreign partners have contributed more than $4 billion to the program's $20 billion development costs.
   Source: http://www.nytimes.com/2006/03/17/business/17fighter.html?_r =1&oref=slogin

7. *March 17, Federal Computer Week* — **Security flaws could cripple missile defense network.** The network that stitches together radars, missile launch sites and command control centers for the Missile Defense Agency (MDA) ground−based defense system has such serious security flaws that the agency and its contractor, Boeing, may not be able to prevent misuse of the system, according to a Department of Defense (DoD) Inspector General's report. The report, released late last month, said MDA and Boeing allowed the use of group passwords on the unencrypted portion of MDA's Ground−based Midcourse Defense communications network. The report said that neither MDA nor Boeing officials saw the need to install a system to conduct automated log audits on unencrypted communications and monitoring systems. The network, which was also developed to conform to more than 20−year−old DoD security policies rather than more recent guidelines, lacks a comprehensive user account management process, the report said.
   Source: http://www.fcw.com/article92640−03−16−06−Web

8. *March 15, Computer World* — **DoD seeks army of cyborg bugs.** The concept of soldier ants may not be far away from a Department of Defense proposal to field an army of remote−controlled insect−cyborg scouts. The Hybrid Insect Micro−Electro−Mechanical Systems program is the responsibility of the Defense Advanced Research Projects Agency, which on Thursday, March 9, announced that it was soliciting research proposals on the technology. These insects would be outfitted with sensors and a wireless transmitter that could enable them to send data on conditions in places inaccessible to human troops. The goal of the program is to produce a sensor−enabled insect with a 100−yard range that could be placed within five meters of a target using electronic remote control and, potentially, Global Positioning System technologies.
   Source: http://www.computerworld.com/networkingtopics/networking/story/0,10801,109580,00.html

[Return to top]

Banking and Finance Sector

9. *March 16, CNET News* — **Banks do battle with debit−card fraud.** Vaults won't repel a new breed of bank robber, which apparently has learned to drain debit−card accounts via electronic thievery. As part of a broader security initiative, Bank of America is offering to alert customers of any suspicious charges or changes to their account via e−mail or text messages almost as soon as they occur. Washington Mutual has also begun offering similar alerts. The new alert system could help customers spot fraud early, which is key to preventing big losses.
Source: http://news.com.com/Banks+do+battle+with+debit−card+fraud/2100−1029_3−6050777.html?tag=nefd.top

10. *March 16, Register (UK)* — **New Trojan captures mouse clicks.** Security researchers have discovered a keylogging Trojan that captures mouse clicks as well as key strokes. PWSteal−Bancos−Q targets customers of online banking and financial institutions primarily in Brazil. However Australian anti−virus firm PC Tools warns that variants could be created to affect additional online financial sites worldwide.
Source: http://www.theregister.co.uk/2006/03/16/mouse_click_capturing_trojan/

11. *March 16, IDG News* — **Coalition calls for action on phishing.** Internet service providers and e−commerce sites can employ more tools to combat phishing scams, including "white lists" of legitimate Websites and using false identification information to scam the scammers, according to a report released Thursday, March 16. The report, published by the National Consumers League and released by a coalition of consumer groups, technology vendors, financial services organizations and law enforcement agencies, also calls on Internet companies to step up their consumer education efforts. Among the more novel techniques recommended by the group was for Internet companies and law enforcement agencies to enter false information, such as bogus credit card numbers, into phishing Websites, allowing police to find phishing scammers by tracking the use of those false numbers.
National Consumers League report:
http://www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf
Source: http://www.infoworld.com/article/06/03/16/76554_HNphishingcoalition_1.html

12. *March 16, Fine Extra Research (UK)* — **U.S. to clamp down on pre−paid cards to fight money laundering.** The U.S. Department of Treasury is planning a crackdown on pre−paid and stored value cards because they are increasingly being used for money laundering purposes, according to a report by Reuters. Unlike normal payment cards, stored value cards can be used to transport large sums of money quickly without being detected and without leaving any kind of 'footprint' or paper trail.
Source: http://www.finextra.com/fullstory.asp?id=15061

13. *March 15, Computer World* — **Ex−GM security guard charged with hacking into company's database.** A former security guard at a General Motors (GM) Corp. technical center has been charged with stealing documents containing the names and Social Security numbers of about 100 GM employees and using those numbers to hack into the company's employee−vehicle database, county police said. The ex−employee, James S. Green, of

Washington Township, MI, then sent e−mails to those employees asking them questions about their vehicles. Green was arraigned Monday, March 13, on eight counts of obtaining, possessing or transferring personal identity information, one count of using a computer to commit a crime and one count of stalking that was unrelated to the GM cases.
Source: http://www.computerworld.com/securitytopics/security/story/0,10801,109583,00.html?SKC=cybercrime−109583

[Return to top]

Transportation and Border Security Sector

14. *March 19, Associated Press* — **Airport briefly halts operations after security breach.** A security breach at Tulsa International Airport resulted in a 75−minute delay in operations on Saturday, March 18. An airport spokesperson says an unidentified man entered one of the airport's concourses without being screened about 2:30 p.m. CST. He did so by using an exit lane that leads from the concourse. Airport officials evacuated the concourse, planes were grounded, and passengers who hadn't boarded their planes had to be rescreened by security.
Source: http://www.kten.com/Global/story.asp?S=4652236&nav=menu410_3

15. *March 19, Security Directory (UK)* — **Heathrow Airport opens fast−track immigration.** Heathrow Airport has opened up a fast−track immigration channel in terminal one; it allows registered passengers to pass through immigration checks using iris scans. Iris Recognition Immigration System or Project Iris also went into operation in terminals two and four in July 2005. Now some UK citizens and a number of foreign visitors will be able to bypass traditional passport checks. After pre−registering, authorized passengers may pass through automated booths on arrival to the UK and have their iris scanned for identification. Data of users' iris patterns are cross−matched with passport details and stored in a secure database.
Source: http://uksecuritydirectory.co.uk/index.php/component/option,com_frontpage/Itemid,73/index.php?option=com_content&task=vi ew&id=187&Itemid=73

16. *March 17, Associated Press* — **FAA plans to extend flight cap at O'Hare.** A cap on the number of flights into Chicago's O'Hare International Airport that was to expire next month will likely be extended until October 28, the Federal Aviation Administration (FAA) announced Thursday, March 16. If the tentative decision stands, it would mark the second time the FAA has extended the 2004 restrictions. When the restrictions were set to expire last October, they were extended until April 1. According to the FAA, if the restrictions were lifted it is likely congestion−related delays at O'Hare −− the most delay prone of the nation's 31 busiest airports when the restrictions were put in place −− would return. FAA spokesperson Tony Molinaro said the restrictions have reduced the number of delayed flights by as much as 30 percent. Under the restrictions, American Airlines, a unit of AMR and UAL's United Airlines, agreed to cut 37 daily peak−hour flights. In addition, domestic airlines are limited to a combined 88 arrivals per hour between 7 a.m. and 8 p.m. CST, down from more than 120 an hour.
Source: http://www.usatoday.com/travel/flights/2006−03−17−ohare−rest rictions_x.htm

17. *March 16, Associated Press* — **Boxcutter prompts evacuation at National Airport.** Passengers in Reagan National Airport's south terminal were evacuated after a security breach

on Thursday, March 16. Transportation Security Administration spokesperson Darrin Kayser said a passenger got through the security checkpoint with a prohibited item. Sources told W*USA 9 News that it was a boxcutter. Security agents were unable to locate the passenger, so everyone was asked to leave the terminal to be re−screened.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=47709

[Return to top]

Postal and Shipping Sector

18. *March 17, DMNews* — **APX Logistics files for Chapter 11.** Third−party logistics provider APX Logistics of Santa Fe Springs, CA, filed for Chapter 11 bankruptcy protection yesterday on Thursday, March 16. APX is the largest Parcel Select mailer partnering with the U.S. Postal Service. Parcel Select is designed for large and midsize shippers wanting a low−cost ground delivery service. Companies save money by mailing sorted parcels closer to their ultimate destination via three levels of entry: bulk mail centers, sectional center facilities or destination delivery units. APX Logistics is the largest of the dozen or so Parcel Select consolidators that specialize in small−package delivery.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3610 8

[Return to top]

Agriculture Sector

19. *March 15, Associated Press* — **Bighorn sheep succumb to disease.** Eight Rocky Mountain bighorn sheep from the Gila National Forest have died since late December from a highly virulent disease that has potential to kill entire herds. Luis Rios, Southwest Area Chief for the New Mexico Department of Game and Fish in Las Cruces, said samples were collected and laboratory tests showed the sheep died from bacterial pneumonia, a disease commonly carried by domestic sheep and goats. Based on a sample group of four mortalities from the 16 collared sheep, bighorn sheep biologist Eric Rominger speculates that a quarter of the 100−plus herd might have died from the disease. The department's goal is to keep bighorn sheep separated from domestic animals to prevent the spread of the disease. But because public lands are often interwoven with private land in New Mexico, it's hard to prevent contact or determine when contact occurred.
Source: http://www.azstarnet.com/dailystar/news/120142.php

[Return to top]

Food Sector

20. *March 15, U.S. Food and Drug Administration* — **Baby food recalled.** H−E−B announced Wednesday, March 15, that it has issued a recall of its entire H−E−B Baby Food and Mom's Organic Choice product lines. As of this afternoon, all H−E−B baby food and Mom's Organic Choice product lines was removed from shelves due to a few customer reports of pieces of glass being found inside the baby food jars of H−E−B peas, carrots, and applesauce.

Source: http://www.fda.gov/oc/po/firmrecalls/heb03_06.html

[Return to top]

Water Sector

21. *March 17, Associated Press* — **Wastewater treatment operator fined.** An Missouri wastewater treatment operator has been fined $25,000 and placed on probation for two years for failing to properly sample discharge from the city of Troy's wastewater treatment facility. Ronald Eisenbath pleaded guilty in January to one count of violation of the Clean Water Act. He was sentenced Thursday, March 16, in U.S. District Court in St. Louis.
Source: http://www.belleville.com/mld/belleville/news/state/14123384 .htm

[Return to top]

Public Health Sector

22. *March 19, Agence France−Presse* — **Bird flu kills Egyptian woman as virus spreads.** Egypt announced Saturday, March 18, a woman had died of the H5N1 strain of bird flu, making her the country's first human victim as the virus spread to birds in neighboring Israel. The woman's death raised alarm in the Middle East, where two other human fatalities resulting from bird flu were already reported in Iraq. Elsewhere in the region, birds have been reported infected with the H5N1 strain of avian influenza in Iran, Israel, and Kuwait. Egyptian state television said the victim, who maintained a domestic bird farm, died of a fever nearly two weeks after she was hospitalized with flu−like symptoms. Egyptian authorities carried out the first tests on the woman, Amal Mohammed Ismail, and passed them on to the Cairo−based U.S. Naval Medical Research Unit (NAMRU) for confirmation.
Source: http://www.forbes.com/home/feeds/afx/2006/03/19/afx2605199.h tml

23. *March 19, Associated Press* — **Israel in mass bird cull.** Israeli veterinary officials on Sunday, March 19, proceeded with the slaughter of hundreds of thousands turkeys and chickens as new tests came close to confirming Israel's first outbreak of the H5N1 strain of bird flu. Agriculture Ministry spokesperson Dafna Varisca said "it's very close to 100 percent" sure that the virus has spread to Israel. She said test results identified hemagglutinin, one of the two proteins in the deadly strain of avian flu. Test results from the second protein, neuraminidase, were still pending, she said. The Cabinet devoted its weekly meeting Sunday to the outbreak, while veterinary officials continued the systematic slaughter of poultry in four farming communities suspected of being hit by the virus. Varisca estimated 400,000 to 500,000 turkeys and chickens would be killed by drinking poisoned water. The flu alert was sounded on Wednesday, March 15, after thousands of turkeys started dying in southern and central Israel. By Thursday, March 16, health officials proclaimed that the disease apparently had hit, and the killing of turkeys began over the weekend as a protective measure.
Source: http://edition.cnn.com/2006/HEALTH/conditions/03/19/bird.flu .israel.ap/

24. *March 18, Reuters* — **U.S. officials hold smallpox preparedness drill.** Top aides to President George W. Bush on Saturday, March 18, looked at ways they might deal with a possible

smallpox attack. White House spokesperson Dana Perino said the drill was one in a series of exercises the administration is holding to look at preparedness for potential public−health disasters. Homeland Security Secretary Michael Chertoff, Health and Human Services Secretary Michael Leavitt, and several other Cabinet secretaries attended the drill. Perino said the aim of Saturday's gathering at the executive building near the White House was to look at federal, state, and local preparedness plans, "identify gaps in preparedness and explore the lessons from Hurricane Katrina in a response that would exceed capabilities at the state and local level."
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−03−18T191221Z_01_N18394136_RTRIDST_0_HEALTH−BUSH−SMALLPOX−DC.XML

25. *March 17, Washington Post* — **Anthrax vaccine won't meet deadline.** The government's effort to develop a new anthrax vaccine has run into difficulty, with the company in charge of the project reporting failure in a major human test and falling at least a year behind schedule. Officers at VaxGen Inc. of Brisbane, CA, said in interviews that they believe they have isolated the problem with their vaccine and are well on their way to fixing it. But they acknowledged that they have no hope of meeting a deadline to deliver 25 million doses of the vaccine into a national stockpile by November and will default on their contract with the government unless it grants an extension they have requested. Until the full stockpile of 75 million doses is ready, the U.S. would depend on antibiotics to treat a large−scale anthrax attack, a strategy that terrorists could overcome by creating antibiotic−resistant anthrax.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/16/AR2006031602285.html

26. *March 17, World Health Organization* — **New tuberculosis strategy launched.** A new strategy to fight tuberculosis (TB) was launched Friday, March 17, by the World Health Organization (WHO). The new “Stop TB Strategy” addresses the current challenges facing countries in responding to TB −− how to continue scaling−up TB control activities while also addressing the spread of TB and HIV coinfection and multidrug−resistant TB (MDR−TB). Both TB/HIV, especially in Africa, and MDR−TB, particularly in Eastern Europe, are seriously hampering global control efforts to reduce the 1.7 million deaths caused by TB every year. At the strategy’s core is DOTS, the TB control approach launched by WHO in 1995. Since its launch, more than 22 million patients have been treated under DOTS−based services. The new six−point strategy builds on this success, while recognizing the key challenges of TB/HIV and MDR−TB.
Tuberculosis information: http://www.who.int/topics/tuberculosis/en/index.html
Source: http://www.who.int/mediacentre/news/releases/2006/pr12/en/in dex.html

27. *March 14, Associated Press* — **Hantavirus case confirmed in Taos County.** New Mexico's third case of hantavirus for 2006 has been confirmed in a Taos County woman. The woman was hospitalized Monday, March 13, at University of New Mexico Hospital in Albuquerque. Health officials were investigating to determine where the woman may have been exposed to the virus. The disease is transmitted through particles of dried urine, droppings or saliva of infected rodents. Earlier cases this year included a woman from McKinley County, who has since recovered, and a Taos man who died from the virus. New Mexico had one case reported last year, in a Los Alamos County man. In 2004, New Mexico had four cases, one each in

McKinley, Bernalillo, Sandoval and Santa Fe counties. The McKinley County case that year was fatal.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.freenewmexican.com/news/40756.html

[Return to top]

Government Sector

28. *March 17, Boston Globe* — **Immigrants arrested as officials target Boston violence.** During a two−day sweep through Boston this week, federal officials arrested 60 immigrants, nearly all with records of arrests or convictions, in what they said was an effort to rid the streets of potential offenders and stem the recent violence that has gripped Boston's neighborhoods. Of the immigrants arrested, 57 had been convicted or charged with crimes ranging from drug−related offenses to rape, kidnapping, and attempted murder, said Matthew J. Etre, acting special agent−in−charge of U.S. Immigration and Customs Enforcement in New England. The sweep marked the largest raid on immigrants with records in New England since the agency was formed three years ago, he said. Forty−three were legal residents, according to Immigration and Customs Enforcement, but legal immigrants are subject to deportation if they have been convicted of a felony. The sweep, dubbed Operation Avalanche, was launched Tuesday, March 14, and finished Wednesday, March 15. The goal was to locate and arrest immigrants whom law enforcement authorities saw as threats to the city, Etre said. Some had been here illegally, while others had been legal residents but were still on the streets despite orders to leave the country after they served prison time.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/03/17/60_immigrants_arrested_as_officials_target_hub_violen ce/

[Return to top]

Emergency Services Sector

29. *March 17, Express−Times (NJ)* — **Cabinet post created for homeland security in New Jersey.** New Jersey Governor Jon Corzine on Thursday, March 16, created a Cabinet−level position of Homeland Security director, to be headed by Richard L. Canas, to replace a patchwork system of agencies that has led to turf battles and missed communication. The agency's primary focus will have one individual coordinating homeland security efforts. The agency will serve as a go−between for the governor's office, state police, local and federal agencies. Canas said his first task will be a complete review of New Jersey's emergency response agencies and recommendations.
Source: http://www.nj.com/news/expresstimes/nj/index.ssf?/base/news−2/1142574905120550.xml&coll=2

30. *March 16, KSDK (MO)* — **Emergency agencies in Missouri call old communications equipment a crisis waiting to happen.** St. Louis, MO, officials say that most emergency responders are currently unable to share critical information. Frank Schaper, executive director of the St. Louis Area Regional Response System, says St. Louis departments have different

radios and are on different frequencies. Police chief Joe Mokwa recently told the St. Louis Police Board, the problem is beyond serious for the region, and it will be expensive to fix. Adding to the communication problem in St. Louis is outdated yet critical equipment.
Source: http://www.ksdk.com/news/news_article.aspx?storyid=93845

31. *March 16, Chicago Tribune* — **Five towns may form 911 dispatch center.** Five DuPage County, IL, communities have begun talks to consolidate 911 calls into one central agency, officials said. Bensenville, Wood Dale, Roselle, Itasca and Addison are looking into forming a regional call center that would dispatch emergency police and fire calls, Bensenville Police Chief Frank Kosman said. A regional 911 agency can lead to greater efficiency in staffing and dispatching of calls to emergency personnel, according to consolidation proponents.
Source: http://www.chicagotribune.com/news/local/nearwest/chi−060316 0254mar16,1,1770606.story?coll=chi−newslocalnearwest−hed

[Return to top]

Information Technology and Telecommunications Sector

32. *March 17, Security Focus* — **Skype Technologies Skype networking routine heap overflow vulnerability.** Skype is prone to a heap overflow vulnerability in its networking routines. Analysis: An attacker who sends a stream of specifically crafted network traffic to a Skype client network can cause the client to overwrite part of the heap, including the heap integrity control data. Since the attacker cannot control the address where the data is written, the most likely effect will be that the Skype will abort execution due to an internal error, although other unpredictable behavior is possible. Such a crash will lead to a loss of availability of the Skype application until it is restarted by the user. A complete list of vulnerable products is available in the source advisory. Solution: A fix for Skype for Pocket PC is not currently available. For further solution details: http://www.securityfocus.com/bid/15192/solution
Source: http://www.securityfocus.com/bid/15192/references

33. *March 17, Washington Technology* — **IT infrastructure protection group appoints leadership.** Major IT companies, systems integrators and associations form the leadership of the Information Technology Sector Coordinating Council established last year. The IT sector council is headed by a 12−member executive committee and chaired by Guy Copeland, vice president of information infrastructure at Computer Sciences Corp. He also is president emeritus of the IT−Information Sharing and Analysis Center, and represents the center within the sector council. The vice chairman of the council is Michael Aisenberg, director of government relations for VeriSign Inc.
Source: http://www.washingtontechnology.com/news/1_1/homeland/28218−1.html

34. *March 16, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−075A: Adobe Macromedia Flash products contain vulnerabilities.** There are critical vulnerabilities in Macromedia Flash player and related software. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Systems affected: Microsoft Windows, Apple Mac OS X, Linux, Solaris, or other operating systems with any of the following Adobe

Macromedia products installed: Flash Player 8.0.22.0 and earlier; Flash Professional 8; Flash Basic; Flash MX 2004; Flash Debug Player 7.0.14.0 and earlier; Flex 1.5; Breeze Meeting Add−In 5.1 and earlier; Adobe Macromedia Shockwave Player 10.1.0.11 and earlier. For more complete information, refer to Adobe Security Bulletin APSB06−03: http://www.macromedia.com/devnet/security/security_zone/apsb 06−03.html
Solution: Apply updates: Adobe has provided the updates for these vulnerabilities in APBS06−03: http://www.macromedia.com/devnet/security/security_zone/apsb 06−03.html
Disable Flash: Please see Microsoft Security Advisory 916208 for instructions on how to disable Flash on Microsoft Windows. For other operating systems and Web browsers, please contact the appropriate vendor.
Microsoft Security Advisory 916208: http://www.microsoft.com/technet/security/advisory/916208.ms px
Source: http://www.uscert.gov/cas/techalerts/TA06−075A.html

35. *March 16, Security Focus* — **Apache mod_ssl CRL handling off−by−one buffer overflow vulnerability.** Apache's mod_ssl is prone to an off−by−one buffer overflow condition.
Analysis: The vulnerability arising in the mod_ssl CRL verification callback allows for potential memory corruption when a malicious CRL is handled. An attacker may exploit this issue to trigger a denial−of−service condition. A complete list of vulnerable products is available in the source advisory. Solution: The vendor has addressed this issue in version 2.0.55 of the 2.0 branch. Users are advised to obtain the available update.
For further solution details: http://www.securityfocus.com/bid/14366/solution
Source: http://www.securityfocus.com/bid/14366/references

36. *March 16, Register (UK)* — **Cybercrime costs businesses more than physical crime.** Cybercrime is more costly to businesses than physical crime, according to a recent IBM survey of 600 U.S. businesses. Lost revenue, wasted staff time dealing with IT security attacks and damage to customer goodwill were rated as a bigger problem than conventional crime by 57 percent of firms in the healthcare, financial, retail and manufacturing industries. Of the respondents in the U.S. finance industry, 71 percent were the most concerned about the threat of cybercrime. According to the IBM survey, 83 percent of U.S. organizations believe they have safeguarded themselves against organized cybercrime but most concentrated on upgrading virus software, improving firewall defenses and implementing patch management systems. IBM said these procedures are a necessary first step but fail to go far enough.
Source: http://www.theregister.co.uk/2006/03/16/ibm_cybercrime_surve y/

37. *March 16, Computer World* — **VeriSign details massive denial−of−service attacks.** A sudden increase in a particularly dangerous type of distributed denial−of−service (DDoS) attack could portend big trouble for companies, according to VeriSign Inc. The attacks, which started on January 3 and ended in mid−February, were notable because they employed an especially devastating kind of DDoS attack, said Ken Silva, VeriSign's chief security officer. Such an attack typically involves thousands of compromised zombie systems sending torrents of useless data or requests for data to targeted servers or networks −− rendering them inaccessible for legitimate use. In this case, attackers sent spoofed domain−name requests from botnets to Domain Name System servers, which processed the requests and then sent replies to the spoofed victims, according to Silva.
Source: http://www.computerworld.com/securitytopics/security/hacking

/story/0,10801,109631,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of several vulnerabilities in Adobe Macromedia Flash products. A system may be compromised if a user accesses a web page that references a specially crafted Flash (SWF) file. Successful exploitation may allow a remote attacker to execute arbitrary code with the privileges of the user. For more information please review the following:

VU#945060 − Adobe Flash products contain multiple vulnerabilities
http://www.kb.cert.org/vuls/id/945060

TA06−075A − Adobe Macromedia Flash Products Contain Vulnerabilities
http://www.us−cert.gov/cas/techalerts/TA06−075A.html

Adobe Security Bulletin: APSB06−03
http://www.macromedia.com/devnet/security/security_zone/apsb 06−03.html

Microsoft Security Advisory: 916208
http://www.microsoft.com/technet/security/advisory/916208.ms px

US−CERT encourages administrators to apply the appropriate updates, patches, or fixes as soon as possible.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 25 (smtp), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 55556 (−−−), 6883 (DeltaSourceDarkStar), 55620 (−−−), 32776 (sometimes−rpc15), 32459 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

38. *March 17, Associated Press* — **Rain threatens more Hawaii dams.** At least two people are dead in Kauai's rugged hills after a century−old dam burst and released a thunderous torrent of water and mud. And with the rain is still falling, officials were closely monitoring the other

earthen dams on the island. In the Waita Reservoir, the water rose past 20 feet, just a few inches short of spilling over. Meanwhile, a dam along the Morita Reservoir, downstream from the dam that broke on Tuesday, March 14, was under dangerous stress as well, officials said. The Army Corps of Engineers and national dam experts were inspecting both, and crews were using pumps to control the water levels at Morita. Nearly all of Hawaii's dams were built early in the past century before federal or state standards, according to Edwin Matsuda, an engineer who heads the state's dam safety programs. Many date to the 1890s, when sugar plantations dotted the islands. Like the dam that burst, many are privately owned earthen structures. Lingle said state law places responsibility for repairing and maintaining reservoirs on private owners but acknowledged that the state was failing in its responsibility to monitor the condition of Hawaii's dams, including the 60 on private property on the Garden Island.
Source: http://www.cbsnews.com/stories/2006/03/16/national/main14116 15.shtml

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer